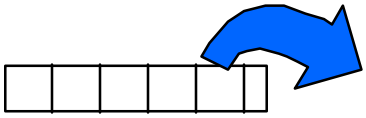
Visualizing Risks:
Icons for Information Attack Scenarios

Hilary H. Hosmer
Data Security, Inc.
Bedford, MA 01730
Email: hosmer@datasecinc.com
Voice and FAX: (781) 275-8231

ABSTRACT

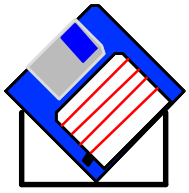
This paper proposes icons and visual conventions for rapid comprehension and presentation of information security (INFOSEC) attack scenario information:


Malicious Intruder


Buffer Overflow


Data Scavenging


Theft


Poorly Installed Software

Attack scenarios describe diverse ways to compromise the security of computer systems and networks. Visual attack scenarios help defenders see system ambiguities, imprecision, vulnerabilities and omissions, thus speeding up risk analysis, requirements gathering, safeguard selection, cryptographic protocol analysis, and INFOSEC training.

The Naval Research Laboratory sponsored this work, a subset of a larger working paper *Visual Conventions for Information Attack Scenarios*,[1] to develop conventions for visualizing INFOSEC scenarios. We recommend follow-up with focus groups.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
16 MAR 2004	**N/A**	**16 Oct 2000 - 19 Oct 2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Visualizing Risks: Icons for Information Attack Scenarios	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Hilary H. Hosmer	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Data Security, Inc. Bedford, MA 01730	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
National Institute of Standards and Technology (NIST) and National Computer Security Center of the National Security Agency (NSA).	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

This paper proposes icons and visual conventions for rapid comprehension and presentation of information security (INFOSEC) attack scenario information: Malicious Intruder, Buffer Overflow, Data Scavenging, QuickTime and a Photo - JPEG decompressor are needed to see this picture. Theft Poorly Installed Software Attack scenarios describe diverse ways to compromise the security of computer systems and networks. Visual attack scenarios help defenders see system ambiguities, imprecision, vulnerabilities and omissions, thus speeding up risk analysis, requirements gathering, safeguard selection, cryptographic protocol analysis, and INFOSEC training. The Naval Research Laboratory sponsored this work, a subset of a larger working paper Visual Conventions for Information Attack Scenarios, 1 to develop conventions for visualizing INFOSEC scenarios.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**18**	

INTRODUCTION

As global connectivity increases, remote terrorists, thieves, spies, pirates, or students can attack remote computer systems aggressively, protected from prosecution by their mobility and position outside national boundaries. Malicious insiders are even more dangerous, thanks to authorized access, on-going opportunity, and intimate knowledge of the systems they attack. Natural disasters, like earthquakes, floods, tornadoes, and electromagnetic phenomena, still wreak devastation on computer systems and networks. Man-made disasters, such as wars, and scientific breakthroughs, such as easy ways to factor large prime numbers, threaten to disrupt secure communications and electronic commerce. Protecting information assets against these threats requires that we understand how they can be attacked.

Figure 1 illustrates two *attack scenarios* featuring a *threat source* (terrorists) with *attack goals (*obtain secrets, money*)*, who employs *threat agents* (hacker and insider) to *attack assets* (money, data) via *vulnerabilities* (Internet and procedural weaknesses) using *attack mechanisms* (e.g. password sniffer) to produce *impacts (*theft of money and data).

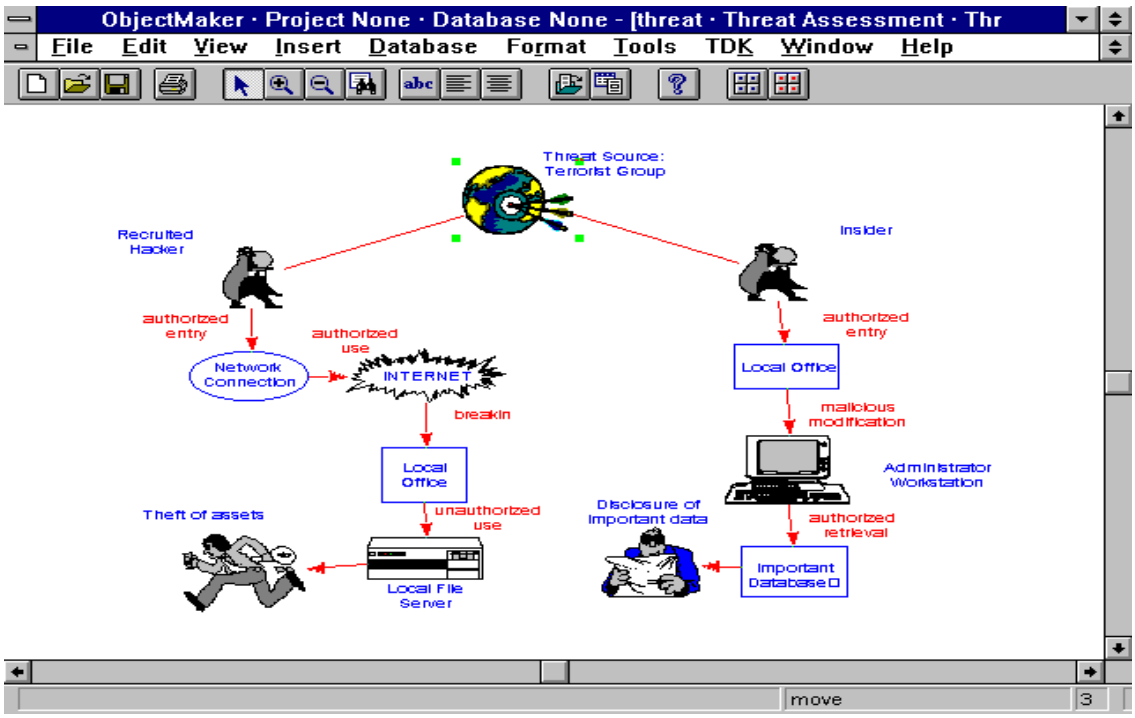


Figure 1: A terrorist group directly attacks one computer site to steal money, and hires an insider to steal secrets from another.[2]

Visualization helps identify missing threats, steps, and safeguards by making potential attack scenarios intelligible to a large number of people. It also helps motivate funding for INFOSEC expenses and to train and motivate personnel to follow INFOSEC procedures.

DEFINITIONS

An information security (INFOSEC) *attack scenario* conveys a way to compromise the security of a computer system or network, from threat source to final impact.

A *language* is a means of communicating ideas and feelings. A *visual language* includes a high percentage of graphic elements to empower the communication.

Symbols, where one thing represents another, are as old as dreams,[3] cave paintings, hieroglyphics, and poetry. They communicate at both cognitive and affective levels.

Icons are graphic symbols. Their power lies in rendering abstract ideas concrete, such as using a flag, logo, or symbol to stand for country, organization, or abstract idea. Common icons include:

Flags

Religions

Money

3.14 15

Love

Frameworks show relationships among components, as in Figure 1. Iconographic "desktop " user-computer interfaces,[4] the *Periodic Table of the Elements*,[5] electronic spreadsheets,[6] and *TCP/IP Protocols Illustrated*,[7] are powerful frameworks for clarifying complexity and promoting innovation. Edward Tufte studied the elements of superior visual frameworks in his books: *Envisioning Information*,[8] and *Visual Explanations*.[9]

Assumptions define the scope of the attack scenario and make implicit concepts explicit. For example, are attackers "rational " (i.e. won't spend more to obtain information than that information is worth). Do they have "deep pockets? "

Resources are financial, technical and sociopolitical capabilities for carrying out attacks.

Constraints limit the use of attack mechanisms and countermeasures. Constraints may be financial, technical, physical, ethical, legal, environmental, or social.

[$5,000,000**]**

Metrics are tools for measurement. They may be:

Numeric (e.g. count, percentage, monetary value);
Non-numeric (e.g. high-medium-low, A-B-C-D-F, one-to-five star ratings);
Fuzzy,[10] non-numeric scales that can be assigned numbers and manipulated mathematically, such as:

Very Skillful (100-80)... Skillful (85-35)...Somewhat Skillful (35-15)...Not Skillful (15-0)

Metrics can be visualized, as shown on the next page.

CRITERIA FOR EFFECTIVE VISUALS

"As for a picture, if it isn't worth a thousand words, the hell with it. "
Ad Reinhardt

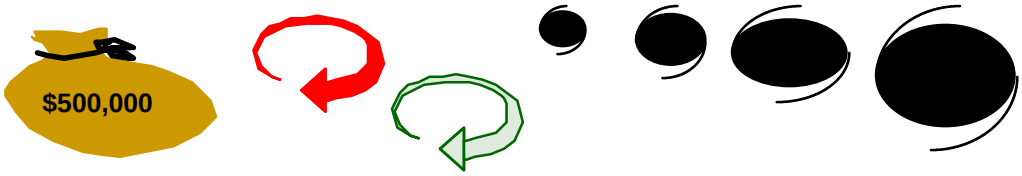
Effective Icons are:

Intuitive, easy to remember, vivid, and easy to use;
Readily available without much effort or expense;
Nonverbal or in English for international usage;
Understandable in both color and black and white;
Reusable in different contexts;
Flexible in size and color;
Performance-sensitive;
Compatible with existing conventions.

Effective Metrics:

Increase accuracy of information;
Enhance quality of information;
Improve comprehension;
May be hidden until needed;
Speed-up decision-making.

Metrics may be put directly on an icon or conveyed using color, texture, scale, or graphs.



Money Social Engineering**:** Hurricane Categories 1-4
Solid = Very Skillful
Dotted = Not Skillful

See Hosmer[11] and Tufte[12] for more extensive visualizing metrics examples.

Effective Frameworks:

Clarify patterns and relationships in a holistic, readily intelligible way;
Are vivid and interesting;
Handle complexity;
Scale upward or downward;
Provide insight into the big picture or details;
Illustrate evolution over time;
Provide a vehicle for effective communication among diverse parties.
Strike a balance between:
Essential concepts and completeness;
Innovation and conformity to existing traditions.

ICONS FOR ATTACK SCENARIOS

ASSET ICONS

Assets are things of value, including hardware, software, data, intellectual property, buildings, equipment, personnel, expertise, procedures, national security, money, and good will. Assets may be classified as *tangible* or *intangible*.

Tangible asset icons:

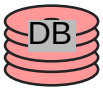
Battleship

Personnel

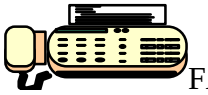
Money

Data

Computer

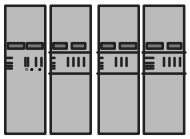


Database



Telephone FAX

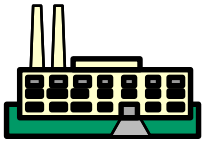
Communications link



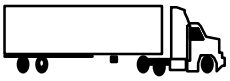
Host Computer

Distributed System

Inventory



Building

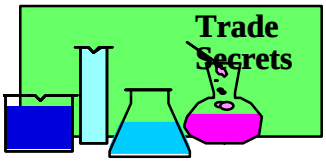


Transport

Intellectual Property Icons:

Patent TM ® ©

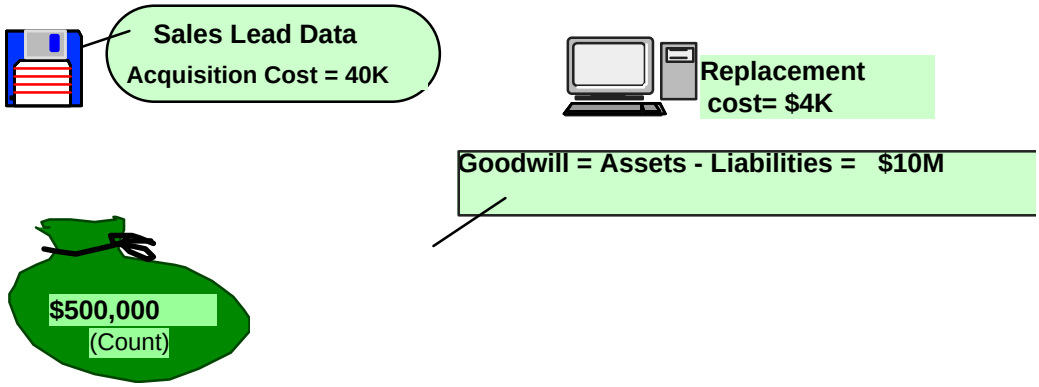
Patent Trademark Registered Trademark Copyright



Intangible asset icons:

Good Will

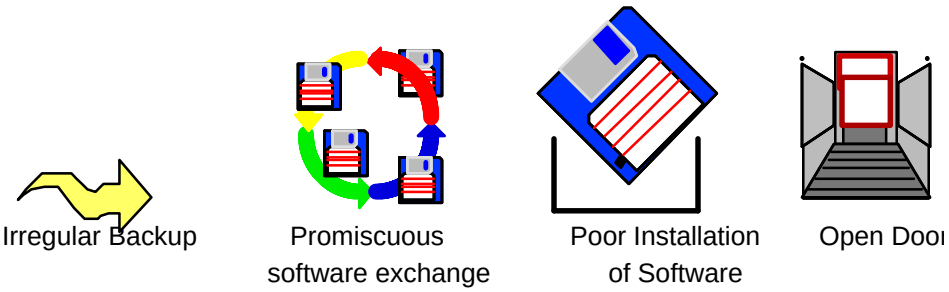
Asset valuation icons, identified by a tag with a light green background, show how much an asset is worth and, optionally, how the worth of the asset was computed.



VULNERABILITY ICONS

Software vulnerabilities:

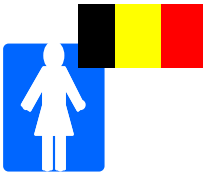
Procedural vulnerabilities:



Personnel vulnerabilities:

In-debt Employee

Disgruntled Employee



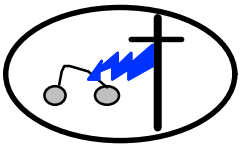
Foreign Employee

Misbehaving Employee

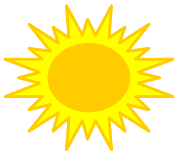
Hardware vulnerabilities:

Magnetism

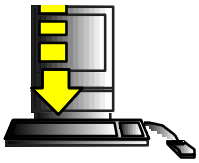
Wiretapping



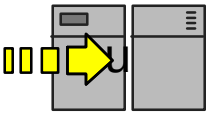
Emanations



Heat



Component Breakdown



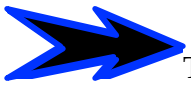
Interface Flaw

Electrical Interference

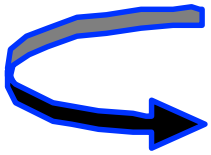
ATTACK ICONS

Attacks are moves on opponents' assets. They may be well-known or novel, overt or covert, passive (e.g. overhearing information) or aggressive (e.g. cutting phone wires).

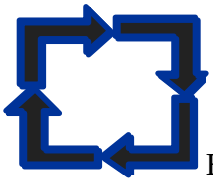
Direct Attack



Two-stage attack (e.g. plant trap-door, then use it later)



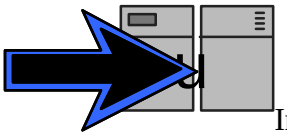
Indirect Attack



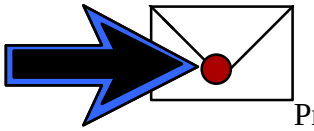
Besiege, Jam, or Control

These may be combined with other icons:

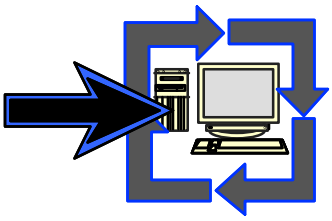
Forgery



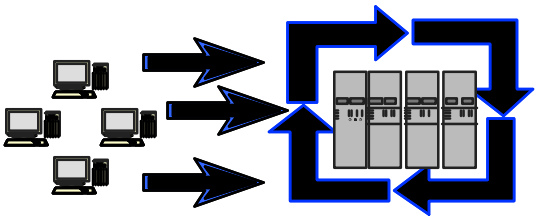
Interface Attack



Privacy Attack



Seize control of system

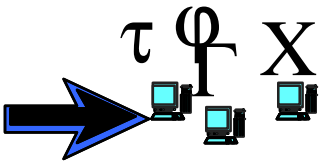


Distributed System Attack

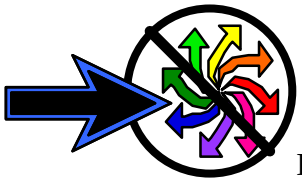
Attacks can also be categorized by their goals or objectives:

Blackmail

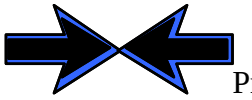
Piracy



Infrastructure Attack



Denial of Service Attack

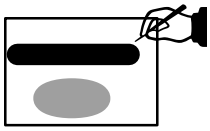


Provocation

ATTACK MECHANISM ICONS

Attackers use *attack mechanisms* to exploit *vulnerabilities.* These may be *physical mechanisms*:

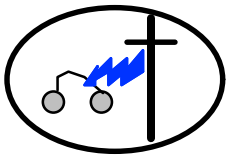
For entering secure areas:



Forged key card

Piggybacking

For data theft:

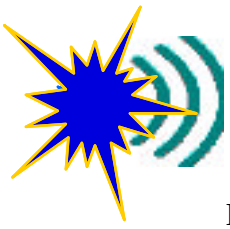


Wiretapping

Steal Data File

For data destruction:

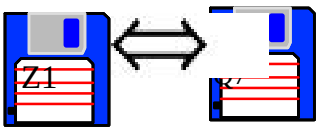
Arson



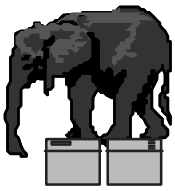
Bomb

Electromagnetic pulse (EMP)

For denial of use:



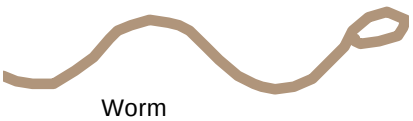
Change file names



Overload Resources

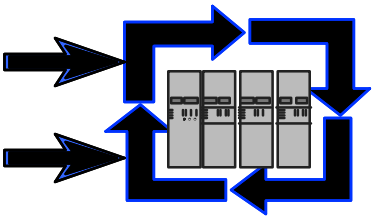
Software attack mechanisms include:

For denial of service:



(Fills computer with code)

Besiege with messages



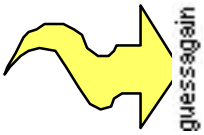
Encrypt others' data:
with unknown key

Sesame

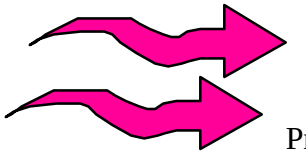
Password

Change others' passwords:

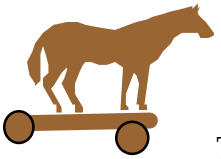
For penetration:



Password Sniffer



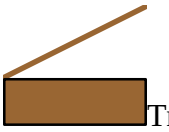
Probes



Trojan Horse

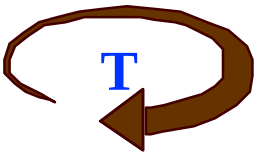
e- 

Electronic Virus



Trap door

For theft using software:



Salami-slicing

Transaction Replay

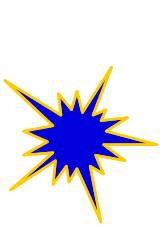
For destruction using software:

e- Logic Bomb

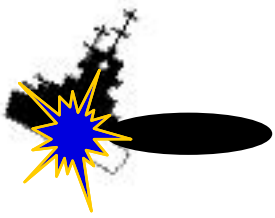
Attack events are specific instances of attacks, such as the Dec. 7, 1941 attack on Pearl Harbor, or the D-Day Allied invasion of Normandy.

World Wide Web site attack
at CIA on 9/22/97 at 2204.22hrs

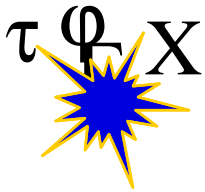
Attack *impacts* are damages (physical, financial, or intangible) to assets.



Damage



Damage to Ship & Environment



Infrastructure Damage

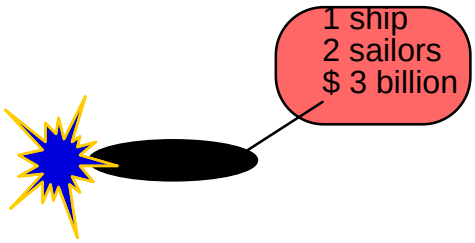
Impacts on assets can be measured. Typical impact metrics include:

Number (e.g. number of personnel, planes or ships lost, months of competitive advantage lost);

Monetary Value (e.g. replacement costs, clean up costs, insurance costs);

Percentage (e.g. market share lost, fall in ratings).

Red ink conventionally means loss.



GOAL AND MOTIVE ICONS

Both *attackers* and *defenders* have physical, financial, or psychological goals.

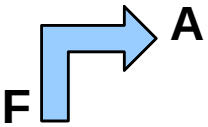
Attackers' objectives:

Steal money

Steal data

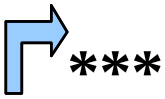
Steal goods

Beat Competitors



Raise Grades

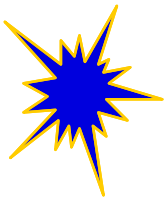
Raise Rating



*

Deny Service

Damage



Attacker motives:

Greed

Visibility/Notoriety

Challenge

Excitement

Power

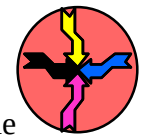
Self-validation

Curiosity

Patriotism

Revenge

Love of Struggle



Defenders’ goals:

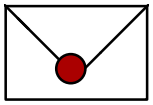
Integrity

Transmission Integrity

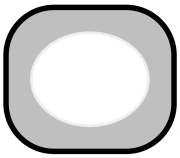
Data Integrity

System Integrity

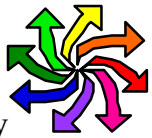
Confidentiality 



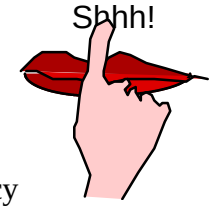
Privacy



Phone Privacy



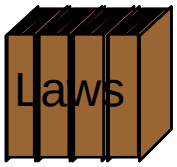
Availability



Secrecy (Personal)

Military Secrecy

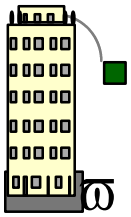
Defenders' motives:



Adhere to Regulations

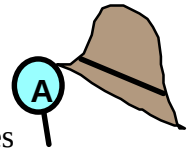
>$ Minimize costs

Enjoy technical challenge



] Limit liability

Solve white collar crimes

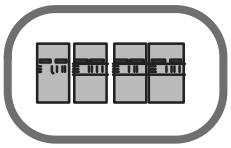


SAFEGUARD ICONS

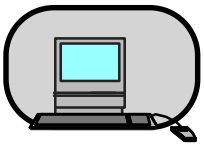
Safeguards and *countermeasures* reduce attack impacts. *Safeguards* protect specific assets while c*ountermeasures* prevent, reduce or mitigate the impact of specific threats by avoiding or transferring risk, reducing vulnerability, recovering quickly, or reducing threat likelihood.

Hardware Safeguards

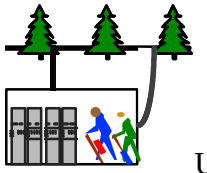
Surge protector



Perimeter Control



Tempest (emanation control)



Underground facility

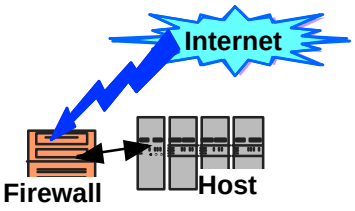
Optical cable

Hardware and Software Safeguards:

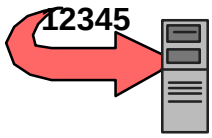
Replicated/Distributed System

Biometric Authentication

Firewall



Data Safeguards:



Back-up Direct data entry Encryption Public and Private Keys

Document Shredder

c 12:23 2/2/00
Time Stamp

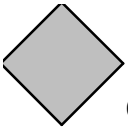
Procedural Safeguards:

Written Procedures

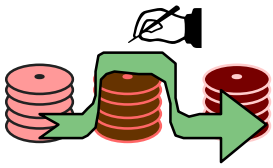
Two-man rule

$ $ Insurance

Poison pill



Official patches



Configuration Management

Security Policy

V&V Validation and verification

NATURAL DISASTER ICONS


Hurricane


Tornado

Water


Dust

Heat


Fire


Eruption


Earthquake


High waves

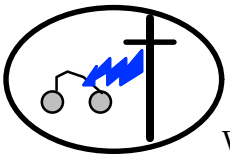

Lightning

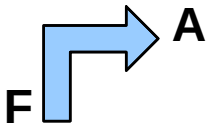
FUTURE WORK

Focus groups would refine these icons, making them appropriate for large groups of people. Additional icons and frameworks are needed to help visualize important INFOSEC applications like medical and e-commerce privacy. We need to more examples of integrating risk analysis metrics into the frameworks.

CONCLUSION

This paper visualized INFOSEC attack scenarios, including threats, assets, attackers' and defenders' goals and motives, system vulnerabilities, attack mechanisms, safeguards and countermeasures, and impacts. To do this we created frameworks, selected existing icons, and created new ones by combining existing fonts, icons, and metrics in new ways with simple artwork. For example:


Wiretapping



Raise Grade

Biometric Authentication

The paper developed criteria for effective icons, frameworks, and metrics, and selected visual conventions to convey many abstract attack scenario concepts. For example:


Spy


Attack

Valuation

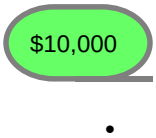
Integrity

These conventions were used in different combinations to convey related concepts:

Reading Emanations

Data Scavenging

Integrity Attack



Valuing Data Integrity

Restrictions on paper length prevented us from including here all the icons and frameworks we developed. Inquiries are welcome.

ACKNOWLEDGEMENTS

Thank you to several colleagues. Maria Green, Katherine Holden, and Bill Ricker reviewed our icons. Bill introduced us to the work of Edward Tufte and Jacques Bertin. Vin McClelland suggested focus groups. Rae Burns, then of Kanne Associates, developed Figure 1 and other iconographic work for an earlier Data Security Inc. Navy Space Warfare Command (SPAWAR) project on graphic CASE tools for threat and risk analysis.[13]

We highly recommend the advanced cryptographic protocol visualization examples from Dr. Jon Graff's *Crypto 101*,[14] designed for "poets, managers, and other mathematically adverse people, " as well as protocols graphics by Catherine Meadows,[15] Bruce Schneier,[16] and W. Richard Stevens.[17]

We used Dr. David J. Stang and Sylvia Moon's taxonomy of risks in *Network Security Secrets*[18] to select common concepts to illustrate.

The icons combine fonts (wingdings, webdings, dingbats, monotype-S and MT-Extra) and MacOS 8.6 library icons. The running figure used for "theft " came from the extensive IMSI Vector Graphics Collection, and the icon for "earthquake " was inspired by the weekly EarthWatch column from the Los Angeles Times.

AppleWorks 5.0 software enabled easy integration of text, drawing, and icons for this paper.

[E]ND NOTES

[1] Hosmer, Hilary H., *Visual Conventions for Information Attack Scenarios*, final report, Data Security, Inc. December, 1999. The Naval Research Laboratory of the Office of Naval Research sponsored this paper under Government Prime Contract N00014-96-D-2024, Subcontract 1400055.

[2] Diagram by Rae Burns of Kanne Associates, produced for SPAWAR SBIR project N00039-96-C-0006 final report *Graphic CASE Tools for Threat and Risk Analysis* by Hilary Hosmer and Rae Burns, ©Data Security, Inc. September 18, 1996.

[3] Jung, Carl G. with M.L. von Franz, Joseph L. Henderson, Jolande Jacobi, Aniela Jaffe, *Man and His Symbols,* Doubleday, New York, 1964.

[4] The Xerox Palo Alto Research Center was the original developer of iconographic user operating system interfaces later adopted by Apple and later Microsoft.

[5] Mendeleeov and Meyer's visual framework, the *Periodic Table of the Elements (1870-1875),* conveys the fundamental properties and interrelationships of chemical elements so effectively, it still appears in most chemistry texts today. Their work enabled understanding of atomic structure and the discovery of missing elements.

[6] The electronic spreadsheet, first developed as VisiCalc in 1979 by Daniel Bricklin, is the application that launched widespread use of the personal computer.

[7] Stevens, W. Richard, *TCP/IP Illustrated, Volume I: The Protocols*, Addison-Wesley, 1994.

[8] Tufte, Edward R., *Envisioning Information*, Graphics Press, 1990.

[9] Tufte, Edward R. *Visual Explanations: Images and Quantities, Evidence and Narrative*, Graphics Press, Cheshire, Connecticut, 1997.

[10] Zadeh, Lofti, originator of fuzzy logic, demonstrated in a large body of work that non-numeric (fuzzy) ranges can be manipulated mathematically.

[11] Hosmer, Hilary H., *Visualizing Risk Metrics*, working paper for NRL, Government Prime Contract N00014-96-D-2024, Subcontract 1400055, 1998.

[12] Tufte, Edward R., *The Visual Display of Quantitative Information*, Graphics Press, 1983.

[13] Hosmer, Hilary, and Rae Burns, *Graphic CASE Tools for Threat and Risk Analysis*, SBIR Final Report for SPAWAR, Data Security, Inc., 1996.

[14] Graff, Jon, *Crypto 101,* KPMG, 1998.

[15] Meadows, Catherine, Fundamental Questions About Formal Methods: Introduction to Panel Discussion, *The Computer Security Foundations Workshop V*, Franconia Inn, June 16-18, 1992, p. 52.

[16] Schneier, Bruce, *Applied Cryptography*, John Wiley and Sons, 1992.

[17] Stevens, W. Richard, *TCP/IP Illustrated, Volume I: The Protocols*, Addison-Wesley, 1994.

[18] Stang, David J. and Sylvia Moon, *Network Security Secrets,* IDG Books Worldwide, Inc. 1993.